

4

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-217861

(43)Date of publication of application : 10.08.2001

(51)Int.Cl. H04L 12/54
H04L 12/58
G06F 13/00

(21)Application number : 2000-022429

(71)Applicant : KDDI CORP

(22)Date of filing : 31.01.2000

(72)Inventor : YAMASHITA KENICHI

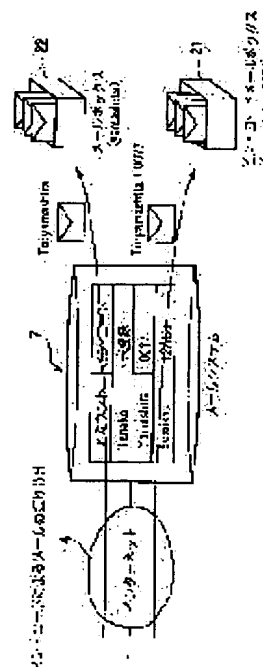
(54) PRANKSTER PREVENTION SYSTEM AND MAIL CENTER SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a system by which users need not receive unnecessary mails with simple operations.

SOLUTION: In the case that a sender user transmits a mail, the user enters a mail address with a PIN code added thereto and transmits the resulting mail. A mail center receiving mails separately stores the received mails with mail addresses having PIN codes to a mail storage memory 21 and stores received logs of mails having mail addresses without PIN codes to a mail storage memory 22.

Thus, reception destination users can read only mails with mail addresses having PIN codes. Furthermore, the reception destination users can read mails, which are sent by the sender users with the mail addresses without the PIN codes through a prescribed operation.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-217861

(P2001-217861A)

(43)公開日 平成13年8月10日(2001.8.10)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード*(参考)
H 0 4 L 12/54		G 0 6 F 13/00	3 5 1 G 5 B 0 8 9
12/58		H 0 4 L 11/20	1 0 1 B 5 K 0 3 0
G 0 6 F 13/00	3 5 1		9 A 0 0 1

審査請求 未請求 請求項の数13 O L (全 16 頁)

(21)出願番号 特願2000-22429(P2000-22429)

(22)出願日 平成12年1月31日(2000.1.31)

(71)出願人 000208891

ケイディーディーアイ株式会社

東京都新宿区西新宿二丁目3番2号

(72)発明者 山下 賢一

東京都港区虎ノ門3丁目5番1号 ディー

ディーアイ東京ポケット電話株式会社内

(74)代理人 100072383

弁理士 永田 武三郎

Fターム(参考) 5B089 GA11 HA10 JA31 KA17 KC28

KC51 KC54 KC58 LA19

5K030 GA15 GA17 HA06 HC01 JT02

JT06 KA06 LD14 LE11

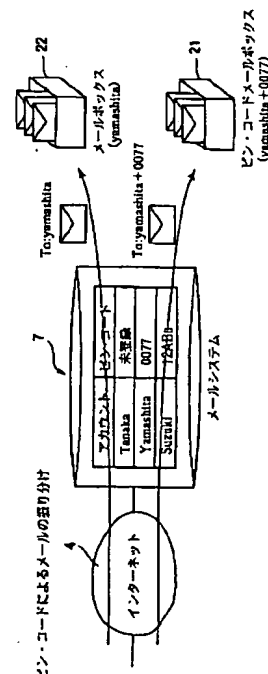
9A001 JJ14 LL03

(54)【発明の名称】 いたずらメール防止システム及びメールセンタ装置

(57)【要約】 (修正有)

【課題】 簡単な操作で不要なメールを受け取らないで済むシステムの提供。

【解決手段】 送信元ユーザがメールを送信する際に、ピン・コードを付加したメールアドレスを入力してメール送信を行う。メールを受信したメールセンタはピン・コード付きメールアドレスで送られたメールをピン・コード付きメール保管メモリ21に、ピン・コードなしメールアドレスのメールは受信ログをピン・コードなしメール保管メモリ22に振り分けて保管する。これにより、受信先ユーザはピン・コード付きメールアドレスで送信されたメールのみを読むことができる。また、受信先ユーザは所定の操作によりピン・コードなしメールアドレスで送信されたメールを読むこともできる。



【特許請求の範囲】

【請求項 1】 ネットワークと接続するメールセンタに該ネットワークを介して送信元ユーザから送信されたメールを保管し、受信先ユーザは所望の時期に前記ネットワークを介して前記メールセンタに保管されているメールを受信可能な電子メール送受信システムにおけるいた

ずらメール防止システムであって、送信元ユーザが、前記メールセンタに登録されている受信先ユーザのあて先コードと共に該受信先ユーザが登録した暗証コードを所定の記述方式で記述してメールを送信した場合には、前記メールセンタはそのメールを受信して第 1 の保管メモリに保管し、

送信元ユーザが、前記メールセンタに登録されている受信先ユーザのあて先コードのみ又は該受信先ユーザが登録した暗証コード以外の文字列を記述してメールを送信した場合には、前記メールセンタはそのメールを受信して第 2 の保管メモリに保管する、ことを特徴とするいた

ずらメール防止システム。【請求項 2】 更に、前記メールセンタは受信先ユーザの通信端末から前記ネットワークを介してメール送信要求があると、前記第 1 の保管メモリに保管されたメールを前記ネットワークを介して前記受信先ユーザの通信端

末に送信することを特徴とする請求項 1 記載のいたずらメール防止システム。【請求項 3】 インターネット又はイントラネットと接続するメールセンタにインターネット又はイントラネットを介して送信元ユーザから送信された送信メールを保管し、受信先ユーザは所望の時期にインターネット又は

イントラネットを介して前記メールセンタに保管されているメールを受信可能な電子メール送受信システムにおけるいたずらメール防止システムであって、送信元ユーザが、前記メールセンタに登録されている受信先ユーザのアカウントに該メールセンタに該受信先ユーザが予め登録したピン・コードを付加したメールアド

レスを用いてメールを送信した場合には、前記メールセンタはそのメールを受信して第 1 の保管メモリに保管し、送信元ユーザが、前記メールセンタに登録されている受信先ユーザのアカウントに該メールセンタに該受信先ユーザが予め登録したピン・コードを付加しないメールアド

レスを用いてメールを送信した場合には、前記メールセンタはそのメールを受信して第 2 の保管メモリに保管する、ことを特徴とするいたずらメール防止システム。【請求項 4】 前記メールセンタは受信先ユーザの通信端末からインターネット又はイントラネットを介してメール送信要求があると、前記第 1 の保管メモリに保管されたメールをインターネット又はイントラネットを介して前記受信先ユーザの通信端末に送信することを特徴とする請求項 3 記載のいたずらメール防止システム。

【請求項 5】 前記メールアドレスは、アカウント+ピ

ン・コード@ドメイン名で記述されることを特徴とする請求項 3 又は 4 記載のいたずらメール防止システム。

【請求項 6】 前記ピン・コードはユーザの通信端末から前記メールセンタに登録し、前記メールセンタに登録済みのピン・コードは該ピン・コードを登録したユーザの通信端末から変更又は削除可能であることを特徴とする請求項 3 乃至 5 のいずれか 1 項に記載のいたずらメール防止システム。

【請求項 7】 前記ピン・コードはユーザの通信端末から前記メールセンタに複数個登録可能であり、前記メールセンタに登録済みのピン・コードは該ピン・コードを登録したユーザの通信端末から変更又は削除可能であることを特徴とする請求項 3 乃至 5 のいずれか 1 項に記載のいたずらメール防止システム。

【請求項 8】 更に、前記メールセンタは受信先ユーザの通信端末からインターネット又はイントラネットを介してログ送信要求があると、前記第 2 の保管メモリに保管されたメール数及び送信元ユーザのメールアドレスをインターネット又はイントラネットを介して前記受信先ユーザの通信端末に送信することを特徴とする請求項 3 記載のいたずらメール防止システム。

【請求項 9】 前記メールセンタは予めユーザの通信端末の電話番号を認証コードとして登録し、電話番号通知機能を用いて取得したユーザ通信端末の電話番号と前記認証コードとを比較してユーザの認証を行うことを特徴とする請求項 3 乃至 8 のいずれか 1 項に記載のいたずらメール防止システム。

【請求項 10】 ネットワークと接続するメールセンタ装置であって、

予めユーザのあて先コードを登録すると共に、ユーザから登録要求があった暗証コードを登録するコード登録手段と、

前記受信先ユーザのあて先コード毎に確保されたメールボックスを有する第 1 のメール保存記憶手段と、

送信元ユーザの通信端末から受信したメールの所定のあて先欄に、送信先ユーザのあて先コードと共に前記コード登録手段に登録されている暗証コードが所定の記述方式で記述されているか否かを判定する判定手段と、

この判定手段により前記暗証コードが送信先ユーザのあて先コードと共に所定の記述方式で記述されていると判定された場合に前記第 1 のメール保存記憶手段に前記メールを保存記憶する記憶制御手段と、

前記送信先ユーザの通信端末からメール送信要求があったとき前記メール保存記憶手段に保存記憶されたメールを取り出して該送信先ユーザの通信端末に送信するメール送信制御手段と、を備えたことを特徴とするメールセンタ装置。

【請求項 11】 更に、ユーザから登録要求のあった暗証コードを前記コード登録手段に登録する暗証コード登録制御手段を備えたことを特徴とする請求項 10 記載の

メールセンタ装置。

【請求項12】更に、前記コード登録手段に暗証コードを登録したユーザから登録済みの暗証コードの変更要求又は削除要求があったとき、登録済みの暗証コードの変更又は削除を行う手段を備えたことを特徴とする請求項10又は11記載のメールセンタ装置。

【請求項13】更に、前記受信先ユーザのあて先コード毎に確保されたメールボックスを有する第2のメール保存記憶手段を備え、

前記記憶制御手段は、前記判定手段により前記暗証コードが送信先ユーザのあて先コードと共に所定の記述方式で記述されていないと判定された場合に前記第2のメール保存記憶手段に前記メールを保存記憶する第2の記憶制御手段を含み、

前記メール送信制御手段は、前記受信先ユーザの通信端末からログ送信要求があると、前記第2の保存記憶手段に保存記憶されたメール数及び送信元ユーザのあて先コードを前記受信先ユーザの通信端末に送信するログ送信制御手段を含むこと、を特徴とする請求項10記載のメールセンタ装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はインターネットやイントラネットにおける電子メール送受信技術に関し、特に、いたずらメールの防止技術に関する。

【0002】

【従来の技術】インターネット上のアンケートやメーリングリストにメールアドレスを登録すると、ダイレクトメールやいたずらメールが送られてくることがある。プロバイダが運営するインターネットメールシステムでは、個人ユーザの多くは電話を利用してメールサーバにダイヤルアップ接続を行っているので、ユーザはメールシステムにある自分のメールボックスに保管されているメールを受信するため、メールの数が多ければメールを読むための電話を接続している時間が長くなり通信料金がかかることとなる。しかも、通常のインターネットメールシステムではいたずらメールであろうがなかろうがメールボックスに保管するので、大量のいたずらメールを保管するとユーザは受信のために多くの通信費用を負担する必要がある。

【0003】そのため、従来、いたずらメールの防止方法として、

① いたずら電話防止策と同様にメールアドレスを変更する方法、

② 通常のメールアドレスとは別にアンケートやメーリングリスト用のアドレスを用意しておき、そのアドレスに送られてくるメールは開かずには消去するといった方法、

③ 図16(a)に示すようにピン(PIN)コード162をメールのサブジェクト(Subject)領域161に

挿入する方法、がある。

【0004】ここで、従来のピン・コードを用いる方法は以下の手順で用いられている。

a：まず、メールの受信者(ユーザ)は自分が所属するメールセンタにピン・コード(暗証番号)を登録する。

b：発信者はサブジェクト領域161に受信者から知らされているピン・コード162を入れてメールを送信する。

c：メールセンタは送信されたメールのサブジェクト領域161に書かれているピン・コード162が予め受信者が登録したピン・コードと一致する場合にのみメールの保管を行う。

【0005】つまり、従来のピン・コード方式を用いたメールシステム、例えば、図16(a)の例に示すように、××社の「suzuki」氏から送られた「TANAKA」氏宛てのメールのサブジェクト領域161には表題の代わりに「TANAKA」氏のピン・コード162(「1234」)が記入されているので、このメールはメールボックスに保管される。これに対し、図16

(b)の例に示すように、〇〇社の「sato」氏から送られた「TANAKA」氏宛てのメールのサブジェクト領域161には予め登録された「TANAKA」氏のピン・コード「1234」でなく表題163(「ゴルフ会員権のご案内」)が記入されているので、このようなメールが送られてもメールボックスに保管されない。

【0006】

【発明が解決しようとする課題】しかしながら、上記①の方法ではメールアドレスの変更はユーザの申し込みに基づいてメールセンタで行うため、ユーザにとってはすぐに変更できないといった不都合があり、メールセンタ側にとっては変更処理に時間や手間がかかるといった問題点があった。

【0007】また、上記②の方法では大量にいたずらメールが送られた場合にユーザがそれらをいちいち消去しなければならず、時間と手間及び接続時間の通信費がかかるといった問題点があった。

【0008】また、上記③の方法ではメールのサブジェクト領域をピン・コード用に使うので、メールに表題を入れることができないためユーザはメールの要件を一瞥して知ることができず、その都度メールの内容を読む必要があるといった問題点があった。

【0009】また、最近のメールシステムの中には予め登録されたキーワードがサブジェクト領域にあると指定のメールアドレスに転送するといった機能を備えたものがあるが、上記③の方法のようにメールのサブジェクト領域にピン・コードを挿入して利用する場合にはこのような機能を利用することができないといった問題点がある(例えば、「緊急」や「至急」と書かれたサブジェクトが含まれていた場合は指定のメールアドレスに転送するようなことができない)。また、ピン・コードの登録

には書面（申込書）を基に登録する方法が一般的であり、一度登録したピン・コードの変更の際も再度書面で変更申し込みを行うことが必要なため変更にかかる時間がかかるといった不都合があった。

【0010】本発明は上記問題点や不都合を解決するためになされたものであり、電子メールシステムにおいて、簡単な操作でいたずらメールやダイレクトメールなどの不要なメールを受け取らないで済むいたずらメール防止システム及びメールセンタ装置の提供を目的とする。

【0011】

【課題を解決するための手段】上記課題を解決するために、第1の発明のいたずらメール防止システムは、ネットワークと接続するメールセンタに該ネットワークを介して送信元ユーザから送信されたメールを保管し、受信先ユーザは所望の時期にネットワークを介してメールセンタに保管されているメールを受信可能な電子メール送受信システムにおけるいたずらメール防止システムであって、送信元ユーザが、メールセンタに登録されている受信先ユーザのあて先コードと共に該受信先ユーザが登録した暗証コードを所定の記述方式で記述してメールを送信した場合には、メールセンタはそのメールを受信して第1の保管メモリに保管し、送信元ユーザが、メールセンタに登録されている受信先ユーザのあて先コードのみ又は該受信先ユーザが登録した暗証コード以外の文字列を記述してメールを送信した場合には、メールセンタはそのメールを受信して第2の保管メモリに保管する、ことを特徴とする。

【0012】また、第2の発明は上記第1の発明のいたずらメール防止システムにおいて、更に、メールセンタは受信先ユーザの通信端末からネットワークを介してメール送信要求があると、第1の保管メモリに保管されたメールをネットワークを介して受信先ユーザの通信端末に送信することを特徴とする。

【0013】また、第3の発明のいたずらメール防止システムは、インターネット又はイントラネットと接続するメールセンタにインターネット又はイントラネットを介して送信元ユーザから送信された送信メールを保管し、受信先ユーザは所望の時期にインターネット又はイントラネットを介してメールセンタに保管されているメールを受信可能な電子メール送受信システムにおけるいたずらメール防止システムであって、送信元ユーザが、メールセンタに登録されている受信先ユーザのアカウントに該メールセンタに該受信先ユーザが予め登録したピン・コードを付加したメールアドレスを用いてメールを送信した場合には、メールセンタはそのメールを受信して第1の保管メモリに保管し、送信元ユーザが、メールセンタに登録されている受信先ユーザのアカウントに該メールセンタに該受信先ユーザが予め登録したピン・コードを付加しないメールアドレスを用いてメールを送信

した場合には、メールセンタはそのメールを受信して第2の保管メモリに保管する、ことを特徴とする。

【0014】また、第4の発明は上記第3の発明のいたずらメール防止システムにおいて、メールセンタは受信先ユーザの通信端末からインターネット又はイントラネットを介してメール送信要求があると、第1の保管メモリに保管されたメールをインターネット又はイントラネットを介して受信先ユーザの通信端末に送信することを特徴とする。

10 【0015】また、第5の発明は上記第3又は第4の発明のいたずらメール防止システムにおいて、メールアドレスは、アカウント+ピン・コード@ドメイン名で記述されることを特徴とする。

【0016】また、第6の発明は上記第3乃至第5のいずれかの発明のいたずらメール防止システムにおいて、ピン・コードはユーザの通信端末からメールセンタに登録し、メールセンタに登録済みのピン・コードは該ピン・コードを登録したユーザの通信端末から変更又は削除可能であることを特徴とする。

20 【0017】また、第7の発明は上記第3乃至第5のいずれかの発明のいたずらメール防止システムにおいて、ピン・コードはユーザの通信端末からメールセンタに複数個登録可能であり、メールセンタに登録済みのピン・コードは該ピン・コードを登録したユーザの通信端末から変更又は削除可能であることを特徴とする。

【0018】また、第8の発明は上記第3の発明のいたずらメール防止システムにおいて、更に、メールセンタは受信先ユーザの通信端末からインターネット又はイントラネットを介してログ送信要求があると、第2の保管メモリに保管されたメール数及び送信元ユーザのメールアドレスをインターネット又はイントラネットを介して受信先ユーザの通信端末に送信することを特徴とする。

【0019】また、第9の発明は上記第3乃至第8のいずれかの発明のいたずらメール防止システムにおいて、メールセンタは予めユーザの通信端末の電話番号を認証コードとして登録し、電話番号通知機能を用いて取得したユーザ通信端末の電話番号と認証コードとを比較してユーザの認証を行うことを特徴とする。

40 【0020】また、第10の発明のメールセンタ装置は、ネットワークと接続するメールセンタ装置であって、予めユーザのあて先コードを登録すると共に、ユーザから登録要求があった暗証コードを登録するコード登録手段と、受信先ユーザのあて先コード毎に確保されたメールボックスを有する第1のメール保存記憶手段と、送信元ユーザの通信端末から受信したメールの所定のあて先欄に、送信先ユーザのあて先コードと共にコード登録手段に登録されている暗証コードが所定の記述方式で記述されているか否かを判定する判定手段と、この判定手段により暗証コードが送信先ユーザのあて先コードと共に所定の記述方式で記述されていると判定された場合

に第1のメール保存記憶手段にメールを保存記憶する記憶制御手段と、送信先ユーザの通信端末からメール送信要求があったときメール保存記憶手段に保存記憶されたメールを取り出して該送信先ユーザの通信端末に送信するメール送信制御手段と、を備えたことを特徴とする。

【0021】また、第11の発明は上記第10の発明のメールセンタ装置において、更に、ユーザから登録要求のあった暗証コードをコード登録手段に登録する暗証コード登録制御手段を備えたことを特徴とする。

【0022】また、第12の発明は上記第10又は第11の発明のメールセンタ装置において、更に、コード登録手段に暗証コードを登録したユーザから登録済みの暗証コードの変更要求又は削除要求があったとき、登録済みの暗証コードの変更又は削除を行う手段を備えたことを特徴とする。

【0023】また、第13の発明は上記第10の発明のメールセンタ装置において、更に、受信先ユーザのあて先コード毎に確保されたメールボックスを有する第2のメール保存記憶手段を備え、記憶制御手段は、判定手段により暗証コードが送信先ユーザのあて先コードと共に所定の記述方式で記述されていないと判定された場合に第2のメール保存記憶手段にメールを保存記憶する第2の記憶制御手段を含み、メール送信制御手段は、受信先ユーザの通信端末からログ送信要求があると、第2の保存記憶手段に保存記憶されたメール数及び送信元ユーザのあて先コードを受信先ユーザの通信端末に送信するログ送信制御手段を含むこと、を特徴とする。

【0024】

【発明の実施の形態】
[いたずらメール防止システムの概要]
図1は本発明のいたずらメール防止システムの概要説明図であり、いたずらメール防止システムはメール送受信機能付き通信端末1（図1の例ではPHSや携帯電話機等のメール送受信機能付き（表示装置付き）無線通信端末1-1、通信機能を備えたパーソナルコンピュータ（以下、パソコン）やモバイル等の情報通信機器1-2、表示装置を備えた電話機やファクシミリ装置等の固定電話装置1-3（これらに限定されない）と、メールセンタ5からなる。また、符号2はインターネット等のネットワークに接続する無線基地局（及びセンタ局）、符号3は交換機、符号4は通信端末1とメールセンタが接続するインターネット等のネットワークを示す。

【0025】送信時に、送信元ユーザはメール送受信機能付き通信端末1を用いて受信先ユーザにメールを送信する際に、図4に示すようにピン・コード（PINコード）を付加したメールアドレス（以下、ピン・コード付きメールアドレス）を入力してメール送信を行う。

【0026】メールを受信したメールセンタ5はメール配信装置10（図2）でピン・コード付きアドレスかピン・コードなしメールアドレスかを調べ、ピン・コード

付きメールアドレスで送られたメールを受信メールとしてメール保管装置20のピン・コード付きメール保管メモリ21（図2）に振り分けて保管し、ピン・コードなしメールアドレスで送られたメールはいたずらメールとして受信ログをピン・コードなしメール保管メモリ22に振り分けて保管する。

【0027】これにより、受信先ユーザはピン・コード付きメールアドレスで送信されたメールのみを読むことができる。なお、受信先ユーザは所定の操作によりピン・コードなしメールアドレスで送信されたメールを読むこともできる。なお、ピン・コードなしメールアドレスで送信されたメールの受信数、送信元のメールアドレスを確認するだけでもよい。また、このようなメールを全てカットする（つまり、ピン・コードなしメールボックスを設けないようにし、ピン・コード付きメールアドレスで送られたメールのみを受信する）ようにしてもよい。

【0028】また、ピン・コード付きメールアドレスはユーザがメール送受信機能付き通信機器1を用いて登録することができ、変更や削除も可能である。すなわち、プロバイダに対する申し込み時には通常のメールアドレス（つまり、ピン・コードなしメールアドレス）で申請し、メールセンタ5側でそのメールアドレスを入力し、登録する。ユーザはこのメールアドレス（ピン・コードなしメールアドレス）にメール送受信機能付き通信端末1を操作してピン・コードを登録し、真に通信を行いたい相手にのみピン・コードを通知することによりいたずらメールを防止することができる。

【0029】また、ピン・コードを複数登録できるようにしてもよい。ピン・コードを1アカウントに対し複数登録することにより事実上そのユーザに複数のアカウントができることになり、目的や相手に応じてピン・コードを設定し連絡しておくことにより、例えば、仕事用、取引先、同僚、友人、親戚別にメールを分別することができる。

【0030】また、通信端末1は表示画面及びメール送受信機能を備えている。通信端末が起動され、ユーザがメール送受信モードを選択するとインターネット4との接続準備動作が行われ、接続するとメールセンタ5からメール送受信モード処理プログラムが通信端末1に転送され、通信端末1は転送されたメール送受信モード処理プログラムをRAM等のメモリに一次的に記憶（ダウンロード）し、その実行制御を行う。

【0031】これにより、図6（a）に示すようなメニュー選択画面が表示される。ユーザがメニュー選択画面に表示されたメニューを選択（ポイント）すると、インターネット4を介して対応するコマンドがメールセンタ5に送られる。また、メール送受信モードが終了するとダウンロードされたメール送受信モード処理プログラムは消去される。

【0032】なお、上記説明ではメール送受信モードが選択される都度、メール送受信モード処理プログラムをメールセンタ5から転送してダウンロードするようにしたが、メールセンタ5からのダウンロードを行わず、通信端末1にメール送受信モード処理プログラムを予めインストールして常駐させるようにしてもよい。

【0033】[メールセンタの構成例]図2はメールセンタ5の一実施例の構成を示すブロック図であり、メールセンタ5はコンピュータ装置からなるメール配信装置10と送信先から送られ、メール配信装置10によって受信されて振り分けられたメールを保管するメール保管装置20から構成されている。

【0034】メール配信装置10は、制御部11、プログラム格納用メモリ12、通信制御部13、送受信部14、キー入力部15、作業用メモリ16、ユーザデータベース17を備えている。また、表示部18、印刷出力部19を備えるようにしてもよい。

【0035】制御部11は、CPU、プログラム格納用メモリ12及びタイマ等の周辺回路を有したマイクロプロセッサ構成を有しており、CPUは上述の各回路及び図示しない電源切換えスイッチ等にバスラインを介して接続し、プログラム格納用メモリ12に格納されている制御プログラムによりメール配信装置10全体の制御を行なうと共に、プログラム格納用メモリ12に格納されているメール配信用プログラム、メール振り分けプログラム、ピン・コード登録・変更プログラム等を取り出して、メール配信、受信メールのメールアドレスのピン・コードの有無による振り分け保存、ユーザ端末からの要求に基づくピン・コードの登録及び変更処理の実行制御等を行なう。また、プログラム格納メモリ12はROM等のメモリからなり、上述した各プログラムのほか通信端末1側に転送するメール送受信モード処理プログラム等や諸定数及びメニューデータを格納することもできる。

【0036】通信制御部13は送受信部14によりインターネット4を介してメール配信装置10とメール送受信機能を備えた通信端末1-1、1-2、1-3等（以下、通信端末1）との間で行うデータ送受信の制御を行う。

【0037】送受信部14は送受信用バッファを備え、通信制御部13の制御下でインターネット4を介して通信端末1との通信制御データ（コマンド）及びメールの送受信処理を行う。また、送受信部14は通信端末1からメールを受信すると発信者電話番号通知機能により発信者電話番号を取得して制御部11に送出する。

【0038】作業用メモリ16はRAM又はDRAM等の一時記憶メモリからなり、プログラムや中間処理結果を一時記憶する。ユーザデータベース17は磁気ディスクやフラッシュメモリ等のリムーバブルな保存メモリからなり、ユーザデータベース領域が確保されている。ま

た、後述するようにユーザデータベース17は契約ユーザのアカウント、ピン・コード（暗証番号）、認証コード（例えば、電話番号）を登録する登録テーブル30からなる。なお、メール配信装置10にユーザデータベース17を設けず、メール保管装置20のメモリにユーザデータベース用領域を設けるようにしてもよい。メール保管装置20は、磁気ディスクや光ディスク等のリムーバブルな大容量高速アクセス可能な保存メモリ装置からなり、メール配信装置10によって振り分けられた、ピン・コードが付加されたメールアドレスのメール（以下、ピン・コード付きメール）を保管するピン・コード付きメール保管メモリ21と、通常（ピン・コードなし）のメールアドレスのメール（以下、ピン・コードなしメール）を保管するピン・コードなしメール保管メモリ22を備えている。また、メール配信装置10からの要求があるとピン・コード付きメール又はピン・コードなしメールを読み出してメール配信装置10に転送する。また、ピン・コード付きメール保管メモリ21とピン・コードなしメール保管メモリ22にはそれぞれ契約ユーザ毎にアカウントで弁別可能に構成されたメール保管領域（メールボックス）が確保されている。なお、図2の例ではピン・コード付きメールボックス21とピン・コードなしメールボックス22を物理的に異なるメモリとして示したが、ピン・コード付きメールボックス21とピン・コードなしメールボックス22を一つのメモリ上で別々の領域に確保するようにしてもよい。

【0039】[ピン付きメールアドレスの構成]通常、メールアドレスは「アカウント@ドメイン名」で表されるが、本発明ではピン・コード付きメールアドレス及びピン・コードなしメールアドレス（＝上述の通常のメールアドレス）をメールアドレスとして扱う。

【0040】ここで、ピン・コード付きメールアドレスは、「アカウント+ピン・コード@ドメイン名」で表される。すなわち、このようにすることにより「アカウント+ピン・コード」はインターネット上でアカウントとして扱われるのでインターネット上でのデータの授受を自在に行うことができる。

【0041】具体的には、送信元ユーザはメールを送る際に受信先のメールアドレスを「アカウント+ピン・コード@ドメイン名」として送信する。なお、記号「+」はピン・コードの前に入力される結合子であり記号「+」に限定されない。また、ピン・コードは受信先ユーザが予めメールセンタに登録した暗証であり、送信元ユーザは受信先ユーザからピン・コードを通知されている。

【0042】なお、実施例ではインターネットのメールアドレスの場合について述べているが、イントラネットでも同様に適用できる。また、ピン・コードをインターネット以外のネットワークのメールアドレスに付加して、いたずらメール防止に適用することもできる（そ

のネットワークにおいて、ピン・コードを付加したメールアドレスがそのネットワークで規定されるメールアドレスとしてそのまま用いられるような方式（或いは記述方法）でピン・コードが付加可能な場合に本発明の適用が可能となる）。

【0043】【ユーザデータベース】図3はユーザデータベース17を構成する登録テーブル30の一実施例を示す図であり、登録テーブル30は、アカウント登録欄31、ピン・コード登録32及び認証コード登録欄33を有している。

【0044】アカウント登録欄31にはメールセンタ5のオペレータによって登録された契約ユーザのアカウントが登録される（図3の例ではアカウントとして、「Tanaka」、「Yamashita」、「Suzuki」が登録されている）。また、ピン・コード登録欄32には後述するようにユーザによるメール送受信機能付き通信端末1の操作によってピン・コード登録操作及びピン・コード（暗証）の入力操作が行われた場合に、入力されたピン・コード（暗証）がメール配信装置10によって登録される（図3の例では、アカウント「Tanaka」のピン・コードは未登録であるが、アカウント「Yamashita」のピン・コードとして「0077」が、アカウント「Suzuki」のピン・コードとして「12AB0」が登録されている）。

【0045】また、変更操作が行われると前回のピン・コードに変更入力されたピン・コードが上書きされ、変更される。また、削除操作によりピン・コード登録欄32からピン・コードが削除される（ピン・コードが登録されていない場合或いはピン・コードが削除された場合にはピン・コード登録欄32は未登録コード（例えば、空白（スペースコード））が書き込まれる）。

【0046】また、認証コード登録欄33には認証コードとして契約ユーザの通信端末1の電話番号がメールセンタ5のオペレータによって登録される。なお、本実施例では後述するようにユーザの認証コード入力の手間を省くために発信者番号通知を利用しているので通信端末1の電話番号を認証コードとして用いているが、これに限定されない（ユーザが通信端末1の操作により設定した認証コードを登録／変更するように構成してもよい）。

【0047】【メールセンタのメール振り分け保管動作】図4はメールセンタ5における受信メールの振り分け動作の説明図であり、図5はメールセンタのメール受信時の動作例を示すフローチャートである。

【0048】ステップS1：（メール送信元ユーザからのメール受信）

メールセンタ5はインターネット4を介して送信元ユーザから送信されたメールを受信し送受信部14の受信バッファに一時記憶する。

【0049】ステップS2：（メールの振り分け）

制御部11は受信メールのメールアドレスを調べ、ピン

・コードが付加されたメールアドレス（アカウント+ピン・コード@ドメイン）の場合にはS3に遷移し、ピン・コードが付加されていないメールアドレス（アカウント@ドメイン）の場合にはS4に遷移する。例えば、図4の例で、「山下」氏宛てのメールのメールアドレスが「Yamashita+0077@abc」の場合にはアカウントにピン・コード「0077」が付加されているのでS3に遷移し、「Yamashita@abc」の場合にはピン・コードが付加されていないのでS4に遷移する。

10 【0050】ステップS3：（ピン・コード付きメールの保管）

制御部11は受信メールをピン・コード付きメール保管メモリ21に確保された受信先ユーザ（契約ユーザ）のメールボックスに保管し、S5に遷移する。また、この際、メールボックスに確保されているメール管理領域に発信元ユーザのメールアドレスを書き込む（メール管理領域に発信元ユーザのメールアドレスと共に発信元ユーザ名、メールの表題を書き込むようにしてもよい）と共にそのメールボックスでの保管メール数をカウントアップする。

【0051】例えば、図4の例では、ピン・コード「0077」が付加されたアカウント「Yamashita+0077」のメールはピン・コード付き保管メモリ21の「山下」氏のメールボックスに保管される。

【0052】ステップS4：（ピン・コードなしメールの保管）

制御部11は受信メールをピン・コードなしメール保管メモリ22に確保された受信先ユーザ（契約ユーザ）のメールボックスに書き込んで保管し、S5に遷移する。また、この際、メールボックスに確保されているメール管理領域に発信元ユーザのメールアドレスを書き込む（メール管理領域に発信元ユーザのメールアドレスと共に発信元ユーザ名、メールの表題を書き込むようにしてもよい）。

【0053】例えば、図4の例では、ピン・コードなしのアカウント「Yamashita」のメールはピン・コードなし保管メモリ22の「山下」氏のメールボックスに書き込まれ、保管される。

【0054】ステップS5：（メール保管通知）

40 メールボックスへのメールの書き込みが終了すると制御部11は送信元ユーザの通信端末にメール保管通知（コマンド）を送信して受信処理を終了する。

【0055】【メールセンタのメール配信動作】

1. ピン・コード付きメールの配信

図6はメール受信先ユーザのメール受信操作時の通信端末側の画面表示の一実施例を示す図であり、図7はメールセンタ5におけるメール配信時の動作説明図である。また、図8はメールセンタのメール配信時の動作例を示すフローチャートである。

50 【0056】ステップT1：（受信ユーザの認証）

ユーザが通信端末1のメール送受信モードを選択すると、インターネット4を介してメールセンタ5との通信接続動作が行われる。制御部11はユーザの通信端末1との通信接続が成立すると発信者電話番号通知機能を利用してユーザ認証を行う。具体的には、接続時に発信者電話番号通知機能により取得した電話番号をキーとしてデータベース17の登録テーブル30の認証コード欄33（実施例では認証コードとして通信端末1の電話番号が予め登録されている（図3参照））を検索し、一致する場合にはメール受信先ユーザとして認証済みとし、図7に示すようにデータベース17の登録テーブル30のアカウント欄31からアカウントを取り出し、T3に遷移する。また、一致する電話番号が登録されていない場合にはT2に遷移する。

【0057】ステップT2：（非認証処理）

上記ステップT2でユーザの認証ができなかった場合には制御部11はその通信端末1に対しての非接続処理（その通信端末に認証不能を意味するメッセージを送信して接続を遮断する等の処理）を行ってメール受信処理を終了する。

【0058】ステップT3：（認証通知等）

制御部11はプログラムROM12からメール送受信モード処理プログラム12を読み出し、通信制御部13を制御して認証済み通知（コマンド）と共に上記ステップT1で認証されたユーザの通信端末1に送信させ、当該通信端末1からのコマンドの受信を待つ。（認証済み通知を受け取った通信端末1はメールセンタ5から送信されたメール送受信モード処理プログラム12をダウンロードして実行する。これにより、図6（a）に示すようなメニュー選択画面が表示される。図6（a）の例で、ユーザが「①メール受信」を選択するとコマンド（メール送信要求を含むコマンド）がメールセンタ5宛て送信される）。

【0059】ステップT4：（選択操作の判定）

メールセンタ5は認証済みユーザ（メール受信先ユーザ）の通信端末1からのコマンドを受信するとその内容を調べメール送信要求が含まれているかを判定し、メール送信要求が含まれている場合にはT5に遷移し、そうでない場合には対応の処理（図5のステップS1、図11のステップU1又は図16のステップV1）に遷移する。

【0060】ステップT6：（ピン・コード付きメール保管メモリの検索）

制御部11は上記ステップT1で認証されたユーザ（メール受信先ユーザ）のアカウント（T1の認証時にデータベース17から取り出したアカウント）をキーとしてピン・コード付きメール保管メモリ21を検索する。

【0061】ステップT7：（保管メール数判定等）

制御部11は上記ステップT6で検索したメールボックスに保管されているピン・コード付きメール数を調べ、

保管メールがある（保管メール数>0）場合にはステップT6に遷移し、保管メールがない場合には通信制御部13を制御してその旨のメッセージ（メール非保管通知（コマンド））を受信先ユーザの通信端末1に送信し、配信動作を終了する。

ステップT7：（メールの送信（配信））

制御部11は上記ステップT6で検索された受信先ユーザのメールボックスのメール管理領域から各ピン・コード付きメールの発信者の送信元情報（メールアドレス（メール管理領域に発信元ユーザのメールアドレス、発信元ユーザ名、メールの表題を書き込むようにした場合にはそれら））と保管メール数を取り出すと共に当該メールボックスに保管されているメールを取り出して送受信部14の送信バッファに転送し、通信制御部13を制御してそれらを受信先ユーザの通信端末1に送信させ、配信動作を終了する。

【0062】上記構成により、図7の例に示すように「山下」氏が自分宛てのメール（アカウント=Yamashita+0077）の受信操作を行うとその電話番号を基に認証が行われ（T1）、通信端末1からメール送信要求が出されると（T4）、ピン・コード付きメール保管メモリ21の検索が行われ（T5）、保管されているピン・コード付きメールだけがユーザ（山下氏）の通信端末1に送信される（T7）。

（メール受信時のユーザの操作及び通信端末の動作）

- ① 受信先ユーザが通信端末1を起動するとインターネット4を介してメールセンタとの接続が開始される。
- ② メールセンタとの接続が確立するとメールセンタ5からメール送受信モード処理プログラムが送信され、ダウンロードされる。そして、そのメール送受信モード処理プログラムが実行され図6（a）に示すような選択メニューが表示される。
- ③ 図6（a）の例で、ユーザがカーソル61で「①メール受信」を選択すると、メール送信要求を含むコマンドがメールセンタ5宛てに送られる。
- ④ メールセンタ5から保管されているピン・コード付きメール数、送信元情報及びメールの送信が開始されると、それらを受信して通信端末1のメモリに順次記憶すると共に図6（b）に示すように保管メール数を表示すると共にメール受信状況を受信済みメール数／保管メール数表示とグラフ表示62で示す（図6（b）の例では帯グラフが示されているが、円グラフ或いは棒グラフでもよい。また、受信メール数の表示だけでもよい）。
- ⑤ メール等の受信が終了すると送信元情報（メールアドレス（メール管理領域に発信元ユーザのメールアドレス、発信元ユーザ名、メールの表題を書き込むようにした場合にはそれら））を一覧表示する。
- ⑥ ユーザは表示された送信元情報の中から図6（c）に示すように所望のメールに対応する送信元情報をカーソル61を用いて選択する。

⑦ 通信端末1はそのメモリに記憶したメールの中からユーザが選択した送信元情報に対応するメール（つまり、ユーザが所望した送信元ユーザからのメール）を取り出して図6（d）に示すように未読件数と共に表示する。

⑧ ユーザは次のメールを読みたい場合には対応する操作ボタンを操作すると、⑤に移行して上述した⑤～⑦の要領で次のメール表示動作が行われる。

【0063】2. ログの配信

図9はメール受信先元ユーザのログ確認時の通信端末側の画面表示の一実施例を示す図であり、図10はメールセンタにおけるログ配信時の動作説明図である。また、図11はメールセンタのログ配信時の動作例を示すフローチャートである。

【0064】前提として、図8でステップT1による認証が行われ、ステップT3で認証通知が出された後、図11のログ配信動作（ステップU1～ステップU4）が実行される。

【0065】ステップU1：（選択操作の判定）

メールセンタ5は認証済みユーザ（メール受信先ユーザ）の通信端末1からのコマンドを受信するとその内容を調べログ送信要求が含まれているかを判定し、ログ送信要求が含まれている場合にはU2に遷移し、そうでない場合には対応の処理（図5のステップS1、図8のステップT1又は図16のステップV1）に遷移する。

【0066】ステップU2：（ピン・コードなしメール保管メモリの検索）

図10で、制御部11は図8のステップT1で認証されたユーザ（メール受信先ユーザ）のアカウント（図8のステップT1での認証時にデータベース17から取り出したアカウント）をキーとしてピン・コードなしメール保管メモリ22を検索する。

【0067】ステップU3：（保管ログ数判定等）

制御部11は上記ステップU2で検索したメールボックスに保管されているログ数（ピン・コードなしメール数）を調べ、保管ログがある（保管ログ数＞0）場合にはステップU4に遷移し、保管メールがない場合には通信制御部13を制御してその旨のメッセージ（ログ非保管通知）を受信先ユーザの通信端末1に送信し、ログ配信動作を終了する。

ステップU4：（ログの送信（配信））

制御部11は上記ステップU2で検索された受信先ユーザのメールボックスのメール管理領域から各ピン・コードなしメールの発信者の送信元情報（メールアドレス（メール管理領域に発信元ユーザのメールアドレス、発信元ユーザ名、の表題を書き込むようにした場合にはそれら））と保管ログ数を取り出すと共に当該メールボックスに保管されているメールを取り出して送受信部14の送信バッファに転送し、通信制御部13を制御してそれらを受信先ユーザの通信端末1に送信させ、配信動作

を終了する。

【0068】上記構成により、図10の例に示すように「山下」氏が自分宛てのログ（アカウント=Yamashita）の受信操作を行うとその電話番号を基に認証が行われ（T1）、通信端末1からログ送信要求が出されると（U1）、ピン・コード付きメール保管メモリ22の検索が行われ（U2）、保管されているピン・コードなしメールがユーザ（山下氏）の通信端末1に送信される（U4）。

10 （ログ確認時のユーザの操作及び通信端末の動作）受信先ユーザの操作及び通信端末の動作中、①、②は図8の場合と同様であり、以下、選択メニュー表示（②）後の動作（③'）から説明する。

③' 図9（a）の例で、ユーザがカーソル91で「③ログ確認」を選択すると、ログ送信要求を含むコマンドがメールセンタ5宛に送られる。

④' メールセンタ5から保管ログ数、送信元情報及びピン・コードなしメールの送信が開始されると、それらを受信して通信端末1のメモリに順次記憶する。また、図9（b）に示すように保管メール数を表示すると共にメール受信状況を受信済みメール数/保管メール数表示とグラフ表示92で示す（図9（b）の例では棒グラフが示されているが、円グラフ或いは棒グラフでもよい。また、メール数の表示だけでもよい）。

⑤' メール等の受信が終了すると送信元情報（メールアドレス（メール管理領域に発信元ユーザのメールアドレス、発信元ユーザ名、メールの表題を書き込むようにした場合にはそれら））を一覧表示する。

⑥' ユーザは表示された送信元情報の中から図9（c）に示すように所望のメールに対応する送信元情報をカーソル91を用いて選択する。

⑦' 通信端末1はそのメモリに記憶したメールの中からユーザが選択した送信元情報に対応するメール（つまり、ユーザが所望した送信元ユーザからのメール）を取り出して図9（d）に示すように未読件数と共に表示する。

⑧' ユーザは次のログを確認したい場合には対応する操作ボタンを操作すると、⑤'に移行して上述した⑤'～⑦'の要領で次のログ確認動作が行われる。

40 【0069】[ピン・コードの登録/変更/削除]図12はユーザによるピン・コード登録操作時の通信端末側の画面表示の一実施例を示す図であり、図13はユーザによるピン・コード変更操作時の通信端末側の画面表示の一実施例を示す図である。また、図14はメールセンタにおけるピン・コード登録/変更/削除時の動作説明図である。また、図15はメールセンタの登録/変更/削除時の動作例を示すフローチャートである。

50 【0070】前提として、図8でステップT1による認証が行われ、ステップT3で認証通知が出された後、図15のピン・コードの登録/変更/削除動作が実行され

る。

【0071】ステップV1：（選択操作の判定）
メールセンタ5は認証済みユーザ（メール受信先ユーザ）の通信端末1からのコマンドを受信するとその内容を調べ、ピン・コードの登録要求、変更要求又は削除信号要求が含まれているかを判定し、ピン・コードの登録要求が含まれている場合にはV2に遷移し、ピン・コードの変更要求が含まれている場合にはV6に遷移し、ピン・コードの削除要求が含まれている場合にはV10に遷移する。また、ピン・コードの登録要求、変更又は削除信号要求のいずれも含まれていない場合には対応の処理（図5のステップS1、図8のステップT1又は図11のステップU1）に遷移する。

【0072】ステップV2：（登録用ピン・コードの取得）

制御部11は受信したコマンドから登録用ピン・コードを取り出す。

【0073】ステップV3：（登録済みの有無判定）

制御部11は図8のステップT1で認証されたユーザ（メール受信先ユーザ）のアカウント（図8のステップT1での認証時にデータベース17のアカウント登録欄31に登録されていたアカウント）に対応するピン・コード登録欄32を調べ、ピン・コードが登録されていない場合はV4に遷移し、既にピン・コードが登録されている場合には登録済みピン・コードと登録済み通知を受信先ユーザの通信端末1に送信し、ピン・コード登録処理を終了する。

【0074】ステップV4：（ピン・コードの登録）

制御部11は上記ステップV2で取得した登録用ピン・コードを上記ステップV3で特定したアカウントに対応するピン・コード登録欄32に書き込む（登録テーブル30のアカウント登録欄31と認証コード登録欄33にはユーザの申し込み時にメールセンタ5側で入力し、登録したアカウント（つまり、ステップV3で特定されたアカウント）及び認証コードが登録されている）。

【0075】ステップV5：（ピン・コード登録通知の送信）

制御部11は上記ピン・コードの登録が終了すると、登録されたピン・コード及び登録通知を送信先ユーザの通信端末1に送信してピン・コード登録動作を終了する。

【0076】ステップV6：（変更用ピン・コードの取得）

制御部11は受信したコマンドから変更用ピン・コードを取り出す。

【0077】ステップV7：（変更前ピン・コードの送信）

制御部11は図8のステップT1で認証されたユーザのアカウントに対応するピン・コード登録欄32（図3）の内容を送信先ユーザの通信端末1に送信する。

【0078】ステップV8：（ピン・コードの変更）

制御部11は上記ステップV7のピン・コード登録欄32に上記ステップV2で取得した登録用ピン・コードを上書きして変更する。

【0079】ステップV9：（ピン・コード変更通知の送信）

制御部11は上記ピン・コードの変更が終了すると、変更後のピン・コード及び変更通知を送信先ユーザの通信端末1に送信してピン・コード変更動作を終了する。

【0080】ステップV10：（データベースの検索及びピン・コードの削除）

制御部11は図8のステップT1で認証されたユーザのアカウントに対応するピン・コード登録欄32（図3）の内容を保持した後、ピン・コード登録欄32の内容を消去する（ピン・コード登録欄32に未登録コード又はスペースを書き込む）。送信先ユーザの通信端末1に送信する。

【0081】ステップV11：（ピン・コード削除通知の送信）

制御部11は保持した消去前のピン・コードを送信先ユーザの通信端末1に送信してピン・コード消去動作を終了する。

【0082】図14は、「山下」氏が登録済みピン・コード「0077」を「0078」に変更した例を示す。この例で、「山下」氏はピン・コード（アカウント=Yamashita+0077）の変更操作を行うとその電話番号を基に認証が行われ（T1）、データベース17の検索及び変更が行われ（V6）、変更通知がユーザ（山下氏）の通信端末1に送信される（U3）。

（ピン・コード登録/変更時のユーザの操作及び通信端末の動作）受信先ユーザの操作及び通信端末の動作中、①、②は図8の場合と同様であり、以下、選択メニュー表示（②）後の動作（③）から説明する。

③” 図12（a）（図13（a））の例で、ユーザがカーソル91で「④PIN・コード登録」（⑤PIN・コード変更）を選択する。

④” 図12（b）（図13（b））に示すような登録用PIN・コード入力案内画面（変更用PIN・コード入力案内画面）が表示されるので、ユーザは図12

（c）（図13（c））に示すように登録用PIN・コード「0077」（変更用PIN・コード「0078」）を入力する。

⑤” PIN・コード登録要求及び登録用PIN・コード「0077」を含むコマンド（PIN・コード変更要求及び変更用PIN・コード「0078」を含むコマンド）がメールセンタ5宛に送られる。

⑥” メールセンタ5からのPIN・コード登録通知（PIN・コード変更通知）を受信すると通信端末1は図12（d）（図13（d））に示すような登録完了画面（変更完了画面）を表示する。

【0083】なお、ピン・コードを複数登録可能にした

場合には、ピン・コード変更の場合には上記ステップV7でそのユーザのアカウントに登録されているピン・コード全てをユーザの通信端末1に送信し、ユーザ側で変更対象のピン・コードを指定して変更対象のピン・コードを含むコマンドを送信し、上記ステップV7とV8の間にそのコマンドを受信するステップと「アカウント+変更対象のピン・コード」をキーとして登録テーブル30を検索するステップを設けることとなる。また、ピン・コード削除の場合にも上記ステップV1とV11の間にそのユーザのアカウントに登録されているピン・コード全てをユーザの通信端末1に送信するステップと、ユーザ側で削除対象のピン・コードを指定して削除対象のピン・コードを含むコマンドを送信したときにそのコマンドを受信するステップと、「アカウント+変更対象のピン・コード」をキーとして登録テーブル30を検索するステップを設けることとなる。

【0084】以上、本発明の一実施例について説明したが本発明は上記実施例に限定されるものではなく、種々の変形実施が可能であることはいうまでもない。

【0085】

【発明の効果】上記説明したように、第1～第4の発明のいたずらメール防止システム及び第10の発明のメールセンタ装置によれば、受信先ユーザのあて先コードにピン・コード等の暗証コードを付加して送信されたメールのみを受信メールとすることができるので、受信先ユーザはいたずらメールやダイレクトメール等のメールを受信することを避けることができる。また、従来のように表題領域にピン・コードを記入するのではなく、あて先にピン・コード等の暗証コードを記述するのでメールの表題を記述することができる。

【0086】また、第5の発明のいたずらメール防止システムによれば、ピン・コードを付加したアカウントを新たなアカウントとしたメールアドレスを構成できるので、インターネット上で自在にメールの送受信を行うことができる。

【0087】また、第6の発明のいたずらメール防止システムによれば、ピン・コードを1アカウントに対し複数登録することにより事実上そのユーザに複数のアカウントができることになり、目的や相手に応じてピン・コードを設定し連絡しておくことにより、例えば、仕事、取引先、同僚、友人、親戚別にメールを分別することができ、いたずらメールの防止により大きな効果を発揮できる。

【0088】また、第7の発明のいたずらメール防止システム及び第11、12の発明のメールセンタ装置によれば、ユーザ側からピン・コードの登録/変更/削除が自由にできるので、ピン・コードの登録が所望の時期にできることに加え、ピン・コードがいたずらメールの送信者に知られた場合などにすばやく変更することもできて従来のようにその都度メールセンタに申し込む必要が

なくなり、取り扱い上ユーザにとって便利となる。

【0089】また、第8の発明のいたずらメール防止システム及び第13の発明のメールセンタ装置によれば、ユーザはログ送信要求を行うことによって、送信メール数や送信元を調べることができるので、いたずらメールやダイレクトメールである可能性の低いメールを読むことができる。従って、例えば、ピン・コードを知らせていなかった知人からのメールや、ピン・コードの変更通知が間に合わなかった人からのメールを読むことができる（つまり、必要なメールをピン・コードが付加されていないというだけで機械的に切り捨てる事態を避けることができる）。

【0090】また、第9の発明のいたずらメール防止システムは電話番号を認証コードとして予めメールセンタに登録し、認証時に、電話番号通知機能を用いて取得された電話番号と登録されている認証コード（電話番号）と比較するので、ユーザは認証コードの設定や入力を行う必要がなく、操作が簡単になる。

【図面の簡単な説明】

20 【図1】本発明のいたずらメール防止システムの概要説明図である。

【図2】メールセンタの一実施例の構成を示すブロック図である。

【図3】ユーザデータベースの登録テーブルの一実施例を示す図である。

【図4】メールセンタにおける受信メールの振り分け動作の説明図である。

【図5】メールセンタのメール受信時の動作例を示すフローチャートである。

30 【図6】メール受信先ユーザのメール送信操作時の通信端末側の画面表示の一実施例を示す図である。

【図7】メールセンタにおけるメール配信時の動作説明図である。

【図8】メールセンタのメール配信時の動作例を示すフローチャートである。

【図9】メール受信先ユーザのログ確認時の通信端末側の画面表示の一実施例を示す図である。

【図10】メールセンタにおけるログ配信時の動作説明図である。

40 【図11】メールセンタのログ配信時の動作例を示すフローチャートである。

【図12】ユーザによるピン・コード登録操作時の通信端末側の画面表示の一実施例を示す図である。

【図13】ユーザによるピン・コード変更操作時の通信端末側の画面表示の一実施例を示す図である。

【図14】メールセンタのピン・コードの登録/変更/削除時の動作説明図である。

【図15】メールセンタ側のピン・コードの登録/変更/削除時の動作例を示すフローチャートである。

50 【図16】従来のピン・コード記入方式によるいたずら

21

メール防止方法の説明図である。

【符号の説明】

- 1 通信端末
 4 ネットワーク、インターネット
 5 メールセンタ（メールセンタ装置）
 11 制御部（判定手段、記憶制御手段、メール送信制

22

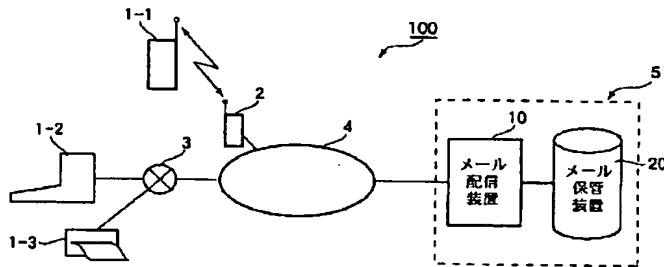
御手段、暗証コード登録制御手段)

21 ピン・コード付きメール保管メモリ（第1の保管メモリ、第1のメール保存記憶手段）

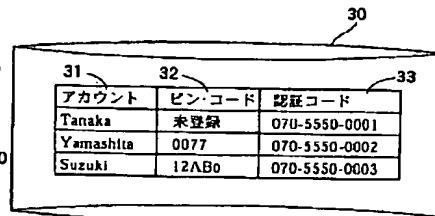
22 ピン・コードなしメール保管メモリ（第2の保管メモリ、第2のメール保存記憶手段）

30 登録テーブル（コード登録手段）

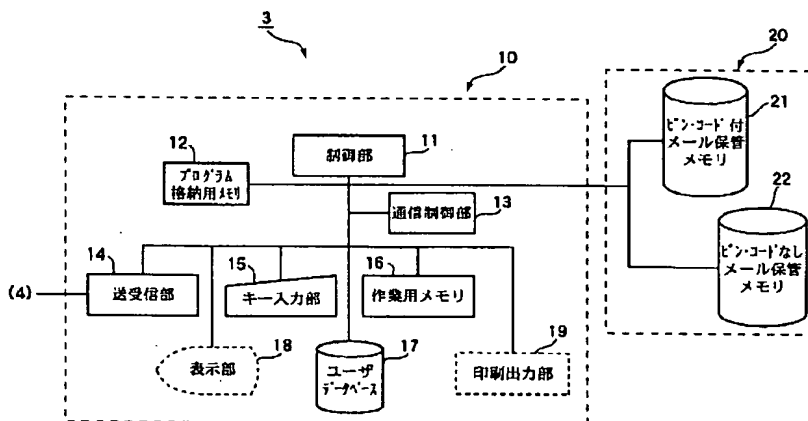
【図1】



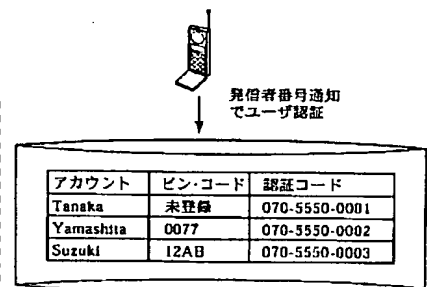
【図3】



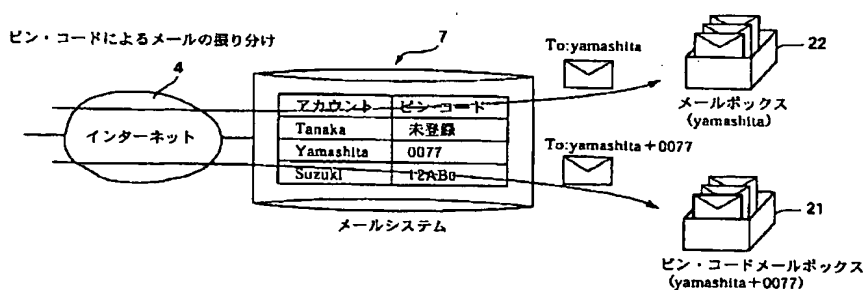
【図2】



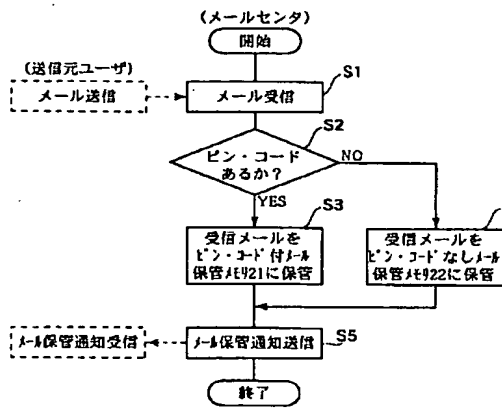
【図14】



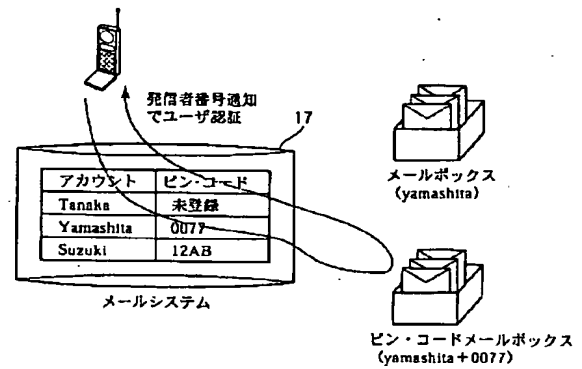
【図4】



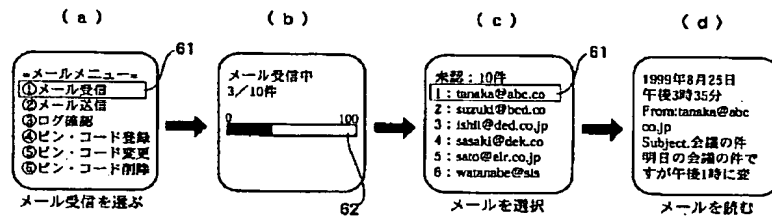
【図5】



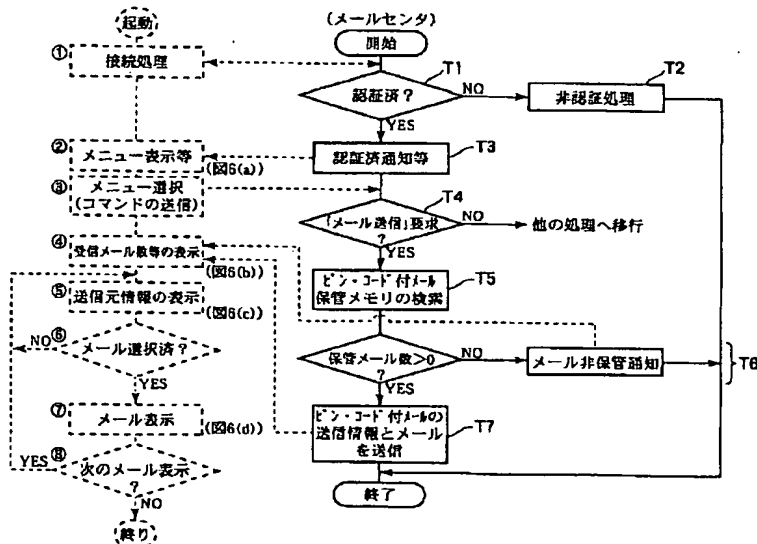
【図7】



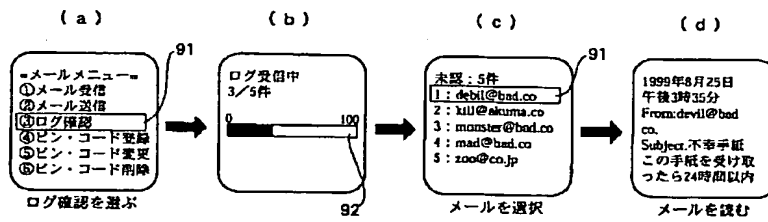
【図6】



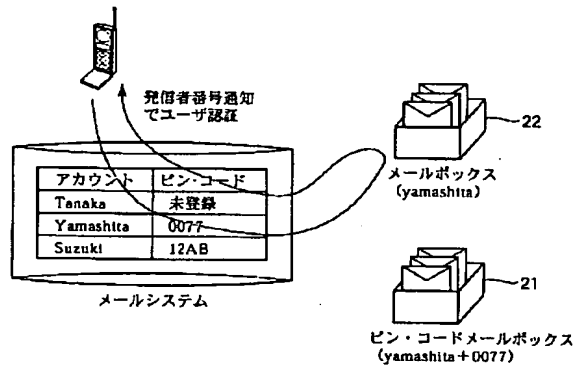
【図8】



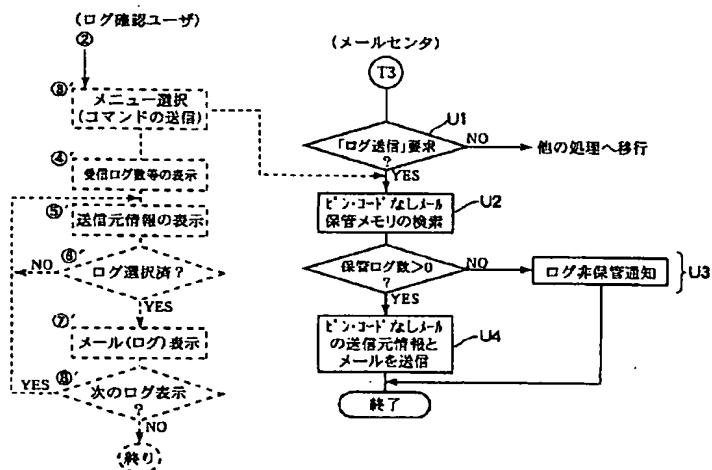
【図9】



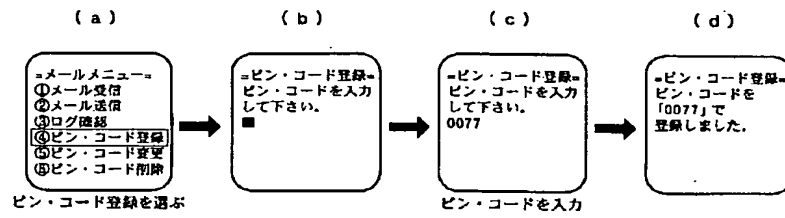
【図10】



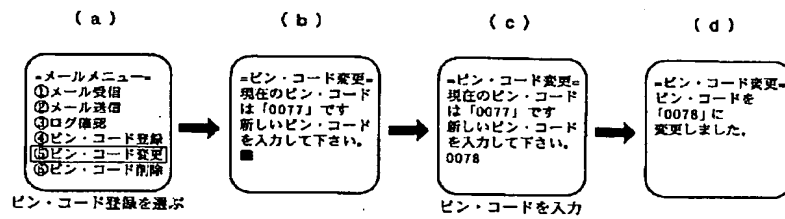
【図11】



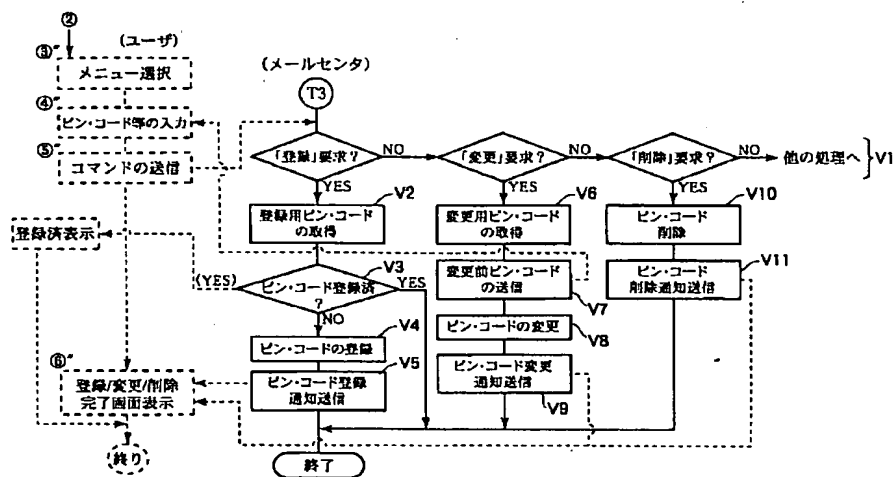
【図12】



【図13】



【図15】



【図16】

